Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Newsletter 31 (2011), 13 December 2011

Unauthorised trading

Banks

Einsteinstrasse 2, 3003 Bern
Tel. +41 (0)31 327 91 00, Fax +41 (0)31 327 91 01
www.finma.ch

A143616/00010/1069215

Contents

1 Introduction

In light of recent cases of unauthorised trading activity, FINMA has decided to detail the application of existing regulations to the management of the risk of unauthorised trading. The recent incident at UBS will not be commented on in this Newsletter.

Operational risks in trading often relate to unreported or unauthorised transactions, incorrect entry of transactions, complex financial instruments, new products or a rapid increase in trading volumes. Such risks have repeatedly led to substantial trading losses for investment banks. The regulatory framework concerning operational risks is provided by FINMA Circulars 08/21 Operational risks – banks, 08/24 Supervision and internal control – banks, 08/7 Outsourcing – banks, and 10/1 Remuneration schemes.

In the application of these existing regulations, FINMA has identified various areas that are important for effective protection against unauthorised transactions. These include corporate governance, the internal control system, reporting, and the outsourcing of control functions. The risk of unauthorised trading transactions is not confined to a small number of individual fields of business, products or systems but is implicit in all trading activities. Institutions engage in a range of different trading activities and thus have different front office and risk systems as well as different control organisations in place. In addition, banks' financial products and fields of business are in a constant state of flux. As a result, the list of requirements below is not exhaustive. However, it summarises FINMA's current expectations for managing the risks associated with unauthorised trading.

2 Corporate governance and control

Senior management should prioritise the risks associated with unauthorised trading appropriately, devoting adequate attention and management resources to identifying, measuring and controlling these risks. In particular, trading activities should be organised such that the risks associated with unauthorised transactions are effectively identified, measured and controlled.

1. The scope, content and intensity of oversight over trading desks must be set out in guidelines. There should be a clear separation of control processes between the front office and downstream control units. This entails in particular defining clear responsibilities and reporting lines.

2. The effectiveness of controls should be subject to the same scrutiny as compliance with earnings targets. As regards the assessment of individual staff, trading desks or business units, this means that indicators for the quality of control activities must be integral to performance measurement and resulting compensation. A balance must be struck between profitability and risk when determining annual goals. A serious violation of rules must lead to disciplinary action.

3. In view of the continual evolution of financial markets, control systems cannot remain static and the continual development of the control system itself must be given priority.

3 Internal controls

Internal control system

4. The internal control system and management information systems must capture all indicators of unauthorised transactions, produce alerts for the responsible control units when preset thresholds are exceeded, and also demand and facilitate a timely, appropriate and effective response. Sufficient human and technical resources have to be available for this purpose. Rules on the escalation of alerts are to be clearly defined.

5. Every trader should have a trading mandate that defines which products may be traded and which strategies pursued. Compliance with the mandate must be checked on an ongoing basis by an independent unit. In particular, traders must not be permitted to approve their own trading activities.

6. Indicators for the risk of unauthorised transactions should be defined and monitored at trader level and, suitably aggregated, escalated to front-office management in order to enable a comprehensive assessment of trader performance. These indicators are to be monitored on an ongoing basis by the downstream control units.

7. The prevailing culture in the front office and downstream control units should encourage a critical attitude as well as professional and responsible conduct. In this connection, it is vital that all control units have sufficient staff and that these staff are sufficiently trained to have an adequate understanding of both the institution’s trading activities they oversee and precise knowledge of the purpose of each individual control. This supports targeted, persistent and critical challenging of trading activities when any potential irregularities are detected. In this respect, it is important that trading offices and control units are within close proximity to each other, an aspect which should be particularly taken into consideration by international banks when organising their trading businesses.

8. Setting up a control dashboard (along with the appropriate governance for its use) where information about all the control functions of a desk or business area (Front Office, Operations, Finance, Risk, Compliance, Treasury, Human Resources, etc.) is regularly recorded is a recommended practice.

9. Regular analysis of the effectiveness of the control system itself is especially important. High quality must be ensured in the implementation of the controls, and this must be checked on an ongoing basis. Checking the effectiveness of controls annually is not sufficient. It must also be ensured that controls are executed to the intended extent and with the intended frequency. All control deficiencies discovered must be escalated immediately. Examples of techniques for revealing weaknesses include scenario analyses, tests of the trading environment for password misuse or unauthorised use of user profiles, or the intentional creation of fictitious bookings. The existing controls must be adjusted in line with the results of these tests. The measures taken to remedy shortcomings should be subject to rigorous quality assurance.

10. A particular challenge arises in the case of staff change, reorganisation or the rollout of a new IT system. Even in phases of transition from an old organisation or IT infrastructure to a new one, it must be ensured that all intended controls are carried out with the required frequency and quality. Additional control measures should be put in place temporarily where necessary. This also applies if control activities are outsourced (see section 5).

11. Staff transfers between related front, middle and back offices should be specially regulated so as to minimise the risk of unauthorised transactions. If staff transfers are permitted, they should be recorded and monitored. Minimum annual holiday requirements must be observed. The relationships between traders and their counterparties should be suitably monitored.

12. Access rights for traders to exchange, booking and settlement systems must be checked regularly in order to establish whether they are commensurate with the assigned trading mandates.

Operational controls

13. In principle, trading positions should be monitored and limited on a gross basis and a net basis. This also applies if only the net positions are ultimately relevant from an economic perspective. Monitoring gross nominal amounts can help to flag up unusual patterns and unauthorised transactions. This principle also applies to risk measures , which should be disclosed, monitored and limited separately for long and short positions – even when only the net risk is economically relevant.

14. In addition to end-of-day values, nominal amounts and risk measures should also be adequately tracked during the trading day and limited on an intraday basis.

15. Where transaction volumes are large, IT-supported routines should preselect transactions for in-depth checking in order to ensure that management can deploy control resources in a risk-oriented manner. In particular, non-standard transactions must be subject to detailed checks. This includes transactions that are not concluded at market prices as well as those that are cancelled, amended or delayed, and those with deferred settlement.

16. In principle, confirmations should be actively sought for all transactions, both external and internal. Outstanding confirmations should be monitored, and unconfirmed transactions should be appropriately escalated. The front office must not inappropriately influence the confirmation process.

17. An independent and robust process for reconciling accounts is essential and should cover both external and internal accounts in full. This also applies to accounts for special purposes (suspense accounts) such as for corrected profit and loss bookings or for booking charges and commissions.

18. Furthermore, the opening and closing of accounts - including inactive accounts - must be explicitly regulated and monitored on an ongoing basis.

19. An independent and robust reconciliation process should exist for margin calls on collateralised transactions.

Profit and loss attribution

20. Explaining how trading profits and losses are generated by trading activities constitutes a key control and serves to improve the understanding of risks associated with trading activities. Large individual profits and losses must be suitably analysed. Larger changes in profit and loss over a specific period (weeks, months, quarters) should also be investigated in detail, and their origin should be explained.

21. The impact on profit and loss of all the transactions that are not concluded at market prices, as well as those that are cancelled, amended or delayed, should be included in the daily and monthly analyses.

4 Internal reporting

22. Internal reporting should allow appropriate monitoring of operational risks in trading. In particular, trading management requires timely information on indicators of operational risks.

23. The reporting system for operational risks should generate alerts automatically as soon as selected indicators exceed preset thresholds.

24. In addition to monitoring and analysing internal indicators, the reporting system for operational risks should systematically capture and evaluate alerts and notices from third parties (staff, exchanges, brokers, clearing houses, custodians, etc.).

25. Reporting must make it possible to analyse profit and loss, liquidity needs and risks of a desk or business area as a whole.

5 Outsourcing

Where controls are outsourced to third parties (within the meaning of FINMA Circular 08/7 Outsourcing – banks, margin numbers 2 and 3), special precautions must be taken to guarantee that the outsourced controls are carried out completely and without interruption.

26. In particular, care must be taken to ensure that the outsourced controls are continued without interruption when the outsourcing partner changes (for example due to a change in staff or IT systems or a reorganisation).

27. Simply checking outsourced controls annually is not sufficient to guarantee that they are carried out completely and without interruption. Instead, the services provided by third parties must be monitored and assessed on an ongoing basis.

28. The company must exercise due diligence in choosing, instructing and controlling the service provider (see FINMA Circular 08/7 Outsourcing – banks, margin number 21).

29. The criteria for selecting and working with a service provider must be determined before entering into a contractual relationship. The service provider must be chosen with due regard to, and subject to checks of, its professional capabilities as well as its financial and human resources. The service provider must offer a guarantee of secure and permanent provision of services (see FINMA Circular 08/07 Outsourcing – banks, margin number 22).

30. The outsourced business area must be integrated into the company's internal control system. A unit within the company must be named as responsible for monitoring and controlling the service provider. The latter's services must be monitored and assessed on an ongoing basis so that any necessary measures can be taken immediately (see FINMA Circular 08/7 Outsourcing – banks, margin number 24).